UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/069,113	06/24/2002	Masayuki Hatanaka	020233	3459

38834 7590 11/07/2006

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 CONNECTICUT AVENUE, NW
SUITE 700
WASHINGTON, DC 20036

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 11/07/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandrie, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/069,113
Filing Date: June 24, 2002
Appellant(s): HATANAKA ET AL.

Andrew G. Melick, Registration No. 56,868
For Appellant

EXAMINER'S ANSWER

This is in response to the Appeal Brief filed 08/18/2006 appealing from the Office action mailed 05/16/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The Brief doe not contain a statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief. Therefore, it is presumed that there are none. The Board, however, may exercise its discretion to require an explicit statement as to the existence of any related appeals and interferences.

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The Appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The Appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

5,392,351	Hasebe et al.	01-1995
5,191,611	Lang	03-1993
2001/0042043	Shear et al.	11-2001

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appeal claims.

Claims 1-5 and 13-18 are rejected under 35 U.S.C. 103(a). The rejection is set forth in prior Office Action dated 01/25/2006 and remains rejected under 103(a) as being unpatentable over prior art of record, U.S. Patent No. 5,392,351 to Hasebe et al ("Hasebe" hereinafter) in view of U.S. Patent 5,191,611 to Lang.

Claims 6-12 are rejected under 35 U.S.C. 103(a). The rejection is set forth in prior Office Action dated 01/25/2006 and remains rejected under 103(a) as being unpatentable over Hasebe et and Lang. and further in view of Shear et at. (US 2001/0042043).

Regarding claim 1: Hasebe discloses a recording device detachably attachable to a reproduction apparatus reproducing and outputting encrypted content data (Hasebe: Col 2, lines 10-15 & lines 27-29), for receiving and recording said encrypted content data therein (Hasebe: Abstract & Col 2, lines 27-29), comprising:

a data input/output unit allowing external data communication; (Hasebe: Col 3, lines 54-56).

a first storage unit receiving said encrypted content data from said data input/output unit for storage; (Hasebe: Col 3, lines 54-56)

a user information hold unit (Hasebe et al., Col. 3, lines 47-56, i.e. personal key generating unit) holding first user ID data provided to identify a user of said recording device; (see also, Hasebe, Figure 2 and associated text, items 13 and 31) a protection information memory unit holding protection information (Hasebe: Col 5, lines 40-45);

a control unit controlling an operation of said recording device, said control unit referring to said protection information to restrict external access to said encrypted content data held in said first storage unit. (Hasebe: Col. 3, lines 47-56, i.e. the decrypting circuit 93, see also, Col 10, lines 50-59 & Col 11, lines 11-19).

Hasebe does not disclose the protection information updatable in response to a result of comparing externally provided user information with said first user ID data.

However, Lang teaches a method to distribute content to different recipients (Lang: Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) to authorize the updating of user information upon successful authorization (Lang: Col 12 lines 36-58).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the updating of protection information after successful authorization is provided. One of ordinary skill in the art would have been motivated to perform such a modification to provide higher flexibility for the users by enabling a subscriber to change the information concerning his authorization to limit or expand his usage (Lang: Col 12, tines 36-58).

Regarding Claims 2, 15 and 17: Hasebe doesn't disclose the device of claim 1, wherein said control unit allows said user ID data to be changed when externally provided user

information and said first user ID data match. However, Lang teaches a method to distribute content to different recipients (See Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) to authorize the updating of user information upon successful authorization (Lang col. 12 lines 36-58).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the updating of protection information after successful authorization is provided. One of ordinary skill in the art would have been motivated to perform such a modification to provide higher flexibility for the users by enabling a subscriber to change the information concerning his authorization to limit or expand his usage (Lang col. 13 lines 29-44).

Regarding claim 3: Hasebe doesn't disclose The device of claim 2, wherein said control unit allows said protection information and said user ID data to be changed when said user information hold unit does not have said first user ID data registered therein. However, Lang teaches a method to distribute content to different recipients (See Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) (Lang col. 12 lines 36-58) and when the user information is not registered enabling the PAD to change user information. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the updating of content information when the user information is not registered in the system yet (Lang: Col 14, lines 5-21). One of ordinary skill in the art would have been motivated to perform such a modification to provide limited access to temporary users or give new users the opportunity to try the system before purchase (Lang col. 14 lines 5-21).

Regarding claim 4: The device of claim 1, wherein said protection information memory unit includes a first protection information memory unit (1520) holding first protection information included in said protection information for restriction on access to said recording device itself, (Hasebe: Col 9, lines 34-45) and said control unit is driven by said first protection information to prohibit additionally recording new encrypted content data in said firs storage unit. (Hasebe: Col 9, lines 46-59).

Regarding claim 5: The device of claim 1, wherein: said protection information memory unit includes a first protection information memory unit holding first protection information included in said protection information for restriction on access to said recording device itself;(Hasebe: Col 10, lines 26-40); and

said control unit is driven by said first protection information to prohibit erasing new encrypted content data in said first storage unit. (Hasebe: Col 9, lines 41-59 / the content is un-rewritable or write-only storage medium is used)

regarding claims 13 and 14: Hasebe discloses the device of claim 1, further comprising a second storage unit (1500) holding license information data corresponding to said encrypted content data, respectively, and required for reproducing said encrypted content data (Col 3, lines 26-39) but he doesn't disclose the control unit is driven by a result of comparing second user ID data externally provided with first user ID data held in said user information hold unit, to control said second storage unit to provide said license information data to said data input/output unit. However Lang teaches a method to distribute content to different recipients (See Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) (Lang: Col 12, lines 36-58) and when there is a match between user

information supplied and the user information stored therein allowing access to the content (Lang: Col 12, line 59 through col. 13 line 8 and Col 13 lines 45-58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the releasing of license information after the authorization of users by comparing their supplied credentials to the one already exist in the system. One of ordinary skill in the art would have been motivated to perform such a modification to limit and track data retrievals by users, as taught by Lang (Col 13 lines 29-44).

Regarding claim 16: Hasebe discloses the device of claim 14, wherein said content user ID data is said first user ID data held in said user information hold unit when said encrypted content data corresponding thereto is distributed. (Col 7, lines 48-62).

Regarding 18: The device of claim 1, wherein said first storage unit is semiconductor memory; and said recording device is a memory card. (COI 3, lines 14-26).

Regarding claims 6 and 7: Hasebe discloses the device of claim 5, wherein: said protection information memory unit includes only one information protection unit (Hasebe: items 1 and 13 of FIG.2) and said control unit driven by first protection information to control access to the content (Hasebe: Col 5, lines 39-45) but he doesn't disclose a second protection information memory unit (1540) holding second protection information for restriction on access for each encrypted content data and the control unit is driven by first and second protection information to prohibit erasing encrypted content data.

However Shear discloses a rights management system for protecting the copying and usage of electronic contents (Shear: Page 3, Paragraph 13) where he teaches using more than one set of security control information (information protection unit) and based on the combination of

one or more of the security control information deciding access level or permitted operation to the content in the storage device (Shear: Page3, Paragraph 34. & 35 and Page 15, Paragraph 214 & 215).

Therefore it would have been obvious to one ordinary skilled in the art at the time the invention was to enable the control unit to decide access based on the data in one or more of the information protection units. One would be motivated to do so in order to enable the content to be used based on one or more proposed electronic agreement (Shear: Page 15, Paragraph 214).

Regarding claims 8, 9 and 10: Hasebe discloses a system as modified above, but he doesn't teach the device of claim 6, wherein when an external instruction is received to effect an operation to reproduce said encrypted content data, said control unit controls said first storage unit and is driven by said second protection information to prohibit producing said data input/output unit with encrypted content data held in said first storage unit.

However Shear discloses a rights management system for protecting the copying and usage of electronic contents (Shear: Page 3, Paragraph 13) where he teaches using more than one set of security control information (information protection unit) (Shear: Page 15, Paragraph 214 & 215) and based on the second protection information deciding the access to the content (Shear: Page 16, Paragraph 220).

Therefore, it would have been obvious to one ordinary skilled in the art at the time the invention was to enable the control unit to use a second protection information when deciding what operation is permitted on a specific content. One would be motivated to do so in order to enable the control unit to prohibit operations on content based on the device trying to use the

content by using the protection information associated with that device (Shear: Page 15, Paragraph 220).

Regarding claim 11: Hasebe discloses a system as modified above, but lacks permitting rewriting on a storage device when there is a match between stored user information and externally provided user information. However, Lang teaches a method to distribute content to different recipients (See Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) to authorize the updating of user information upon successful authorization (Lang col. 12 lines 36-58). Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to enable the rewriting of information to the storage medium after successful authorization is provided. One of ordinary skill in the art would have been motivated to perform such a modification to provide higher flexibility for the users by enabling a subscriber to update or use his information after providing successful authentication (Lang col. 13 lines 29-44).

Regarding claim 12: Hasebe discloses a system as modified above, but lacks permitting rewriting on a storage device when the user ID is not registered in the device. However, Lang teaches a method to distribute content to different recipients (See Abstract) where he teaches comparing stored users information with the user information supplied by a personal access device (PAD) (Lang col. 12 lines 36-58) and when the user information is not registered enabling the PAD to change user information. Therefore it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable the rewriting of content information when the user information is not registered in the system yet (Lang: Col 14, lines 5-

21). One of ordinary skill in the art would have been motivated to perform such a modification to provide limited access to temporary users or give new users the opportunity to try the system before purchase (Lang col. 14 lines 5-21).

(10) Response to Argument

Appellant has argued that Hasebe in view of Lang does not teach or suggest "a user information hold unit," "a control unit," a protection information memory unit," and "a recording device detachably attachable to a reproduction apparatus" as recited in claim 1 (Appeal Brief pages 8-9).

Appelant has further argued that the Hasebe's personal key generating unit generating a personal number is not information identifying a user, thus the personal key generating unit of Hasebe is not an information hold unit for identifying a user of a recording device as recited in claims 1 (Appeal brief bottom of page 8 bridging onto page 9).

The Examiner responds that Hasebe does disclose that (col. 3, lines 23-26) "[T]he user's computer includes the user's personal number 91" and that Hasebe's personal number is processed into a personal key . That is, Hasebe's user computer includes user's personal number 91 and the personal key generating unit (col. 3, lines 47-56, see also col. 7, lines 56-57) processes the user's personal number 91 into a personal key.It is the position of the Examiner that Hasebe's personal number 91 which identifies the user's computer (recording device) is clearly associated with both the user and the computer.

As per Applicant's arguments relating to claimed "control unit" , the applicant argues (Appeal brief, pages 10-11) that "decrypting unit 93 of Hasebe does not control the operation of

the recording device" and that in the present invention, "protection information, such as reproduction flag, is reffered to before proceeding to decryption of the encrypted data" .

The Examiner responds that the decrypting unit 93 of Hasebe reads on the claimed contol unit, because the decrypting unit 93 controls the operations of the Hasebe's recording device by decrypting the permission information 71 from the software storage medium 71 based on the personal key. In response to Appellant's argument that the references fail to show certain features of Appellant's invention, it is noted that the features upon which Appellant relies (i.e., *"reproduction flag, is reffered to before proceeding to decryption of the encrypted data "*) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

As per Appelant's argument realting to "a protection information memory unit holding protection information ", the Appelant has argued that Hasebe's permission informatin 13 does not correspond to the claimed protection information because the premmision information 13 of Hasebe is not information such as wherether or not additional recoding is allowed, whether or not data is erasable, and whether or not data is reproducible (Appeal Brief, page 13, last paragraph).

The Examniner responds that such detailed description of the claimed "protection information" is not recited in the rejected claims. Appelant has further argued that Lang does not disclose that protection information is updatable in response to a result of comparing externally provided user information with the first user ID data, as edxternally provided because in the lang the information provider gives the user an updated access code whereas in the claimed invention

the user controls the protection of information on the recording device. This feature, again, is not recited in the rejected claims.

Appelant has argued (Appeal Brief, pages 14-15) that Hasebe in view of Lang does not teach or suggest " a recording device detachably attachable to a reproduction appratrus." and that the present invention "relates to a memory card ".

In response to Appelant's arguments, the recitation "a recording device detachably attachable to a reproduction appratrus" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535 F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Therefor, claims 1-18 stand rejected over Hasebe in view of Lang.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

November 2, 2006

Conferees

Primary Examiner
Kambiz Zand

Supervisory Examiner
Kim Vu

Primary Examiner
Taghi T. Arani

WESTERMAN, HATTORI, DANIELS & ADRIAN, LLP
1250 Connecticut Ave., NW
Suite 700
Washington, DC 20036